



Federal Trade Commission

“Promoting Consumer Privacy: Accountability and Transparency in the Modern World”

**Remarks of David C. Vladeck, Director, FTC Bureau of Consumer Protection¹
New York University
October 2, 2009**

I. Introduction

Science-fiction writer David Brin once said, “when it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else.” Well, as policymakers, we must demand privacy and accountability from everyone. Certainly, businesses and governments must be held accountable: They must respect consumers’ privacy in collecting and using data. But individuals also have to take responsibility for the data they share, including the data they post on the Internet.

However, before we can hold consumers accountable in this way, we also need to promote transparency of privacy practices. Consumers need to understand how the information they share will be used, so that they can make informed decisions about whether to share it in the first place. In short, along with accountability for information practices, we need to promote transparency and ways of enabling consumers to exercise meaningful choice.

¹The views stated here are my own and do not necessarily reflect the views of the Commission or any Commissioners.

The Federal Trade Commission is assessing the best ways to promote transparency and accountability in commercial information-handling practices. To this end, we are launching a project to explore new consumer privacy frameworks. As part of this project, the Commission will host a series of roundtables to get public input on various models for promoting consumer privacy. The first such roundtable will take place on December 7 at FTC Headquarters in Washington, D.C. I invite all of you to attend.

In my remarks today, I'll take a look at the Commission's past privacy initiatives and discuss how they will inform the future. I'll start by briefly discussing the evolution of the Commission's privacy program over the past decade. I'll then discuss some of the lessons we've learned from our most recent initiatives on privacy and how we will apply those lessons in our effort to explore new consumer privacy

The privacy concerns also have evolved. Some of you may have read the piece in last Sunday's New York Times magazine about middle-schoolers struggling with their sexual orientation. Take the example of one of the adolescents in the article who didn't want to state publicly that he was gay. Suppose he wanted to find information about others in his situation. Just a generation ago, he may have gone to his local library to find this information in the encyclopedia, and emerged with no record of his search. That effort would be anonymous, and would leave no paper trail. There was no privacy debate to be had.

Today, the individual would probably look for information on the Internet. If he does so on his home computer, he may be surprised — indeed, even mortified — to receive advertising based on his searches and to learn that third parties have access to information about his searches. Even if the individual conducts his search at the local library or on a public computer, there may be a record of that search that may be used in ways he did not and probably could not anticipate — after all, he may have had to enter his library card information or credit card number to access the Internet. As this simple example shows, the privacy implications of new technologies are vast.

This example also shows why our policies need to be adaptable. We may not like the fact that our Internet research can be tracked. But I don't think that even the most privacy-sensitive person among us would advocate for going back to the days of library-based encyclopedia resea

to address behavioral advertising. Behavioral advertising benefits consumers in the form of advertising that is more relevant to their interests. It also helps to subsidize and support a diverse range of free online content and services that otherwise might not be available or that consumers would otherwise have to pay for – content and services such as blogging, social networking, and instant access to newspapers and information from around the world.

At the same time, however, behavioral advertising raises consumer privacy concerns. For one thing, it is far from clear that consumers even know that they are being “tracked” when they visit internet sites. And those consumers who understand tracking, may be uncomfortable with being tracked, but may be unable to engage in self-help. In addition, without adequate safeguards in place, consumer tracking data may fall into the wrong hands or be used for unanticipated purposes. These concerns are exacerbated when the tracking involves sensitive information about, for example, children, health, or a consumer’s finances.

In November 2007, the FTC held a “Behavioral Advertising” Town Hall to explore the impact of new developments in this area. Based upon the discussions at the Town Hall, FTC staff issued for public comment a set of high-level proposed principles to encourage and guide industry self-regulation.² This February, we issued a report that responded to the comments received and fleshed out the principles further.³ The Town Hall, principles, and report contain several lessons for our ongoing work to explore new privacy frameworks.

A: Lesson 1: Timing is Everything

² See Federal Trade Commission, “Behavioral Advertising: Tracking, Targeting, & Technology,” available at <http://www.ftc.gov/bcp/workshops/behavioral/index.shtml>.

³ See Press Release, “FTC Staff Revises Online Behavioral Advertising Principles,” Feb. 12, 2009.

Vijayan, Jaikumar, "Privacy Advocates Hail Facebook's Plan to Shutt

information is collected and shared with third parties. The Beacon example is one example of this. Another example is the rise of third-party applications – because the use of third-party applications on social networking sites is relatively new, many consumers may not be familiar with how such applications could gain access to their data.

Similar challenges arise in the area of P2P file sharing. Recent news reports have highlighted disturbing instances of sensitive documents being shared via P2P networks. These have included documents disclosing avionics details of the President’s helicopter,⁵ financial information of a Supreme Court Justice,⁶ and many thousands of tax returns and medical records of ordinary citizens.⁷ In this context, consumers may download P2P software to share music files, knowing that their music files are accessible to others. The consumers (or perhaps more often, their teenage children) might not know, however, that the software can give people access to *all* of the personal data from their computers.

Just like consumers, businesses need guidance on how to protect consumer privacy in the face of new technological developments. For example, as screens get smaller, how do businesses provide adequate disclosures to consumers about privacy issues? I can barely read messages on my Blackberry or cell-phone. And as responsibility for data protection becomes more diffuse – as in the case of cloud computing, where invisible service providers may remotely process and store data – who is responsible for safeguarding it?

⁵ Cooper, Charles, “Data About Obama’s Helicopter Breached Via P2P?” CNET News, Feb. 28, 2009, <http://news.cnet.com/data-about-obamas-helicopter-breached-via-p2p>.

⁶ Krebs, Brian, “Justice Breyer is Among Victims of Data Breach Caused by File Sharing,” Washington Post, A01 (July 9, 2008).

⁷ Sandoval, Greg, “Congress to Probe P2P Sites Over ‘Inadvertent Sharing’” CNET News, Apr. 21, 2009, http://news.cnet.com/8301-1023_3-10224080-93.html.

Moreover, the timing is right to reexamine privacy issues, not only because of advances in technology, but also because of advances in innovative policymaking. We need to take advantage of the momentum that is building around in the United States and around the globe on privacy issues. The House Energy and Commerce Committee is drafting new omnibus privacy legislation, and the Administration is convening meetings to develop positions on privacy. In addition, the new Business Forum on Consumer Privacy, consisting of business leaders from Microsoft, eBay, Google, and Hewlett Packard, has recently formulated a new approach to protecting privacy in the digital economy. And the Ontario Privacy Commissioner has launched a “Privacy by Design” Challenge, through which it has called on companies to embed privacy-enhancing technologies into the architecture of new systems. There is a lot of creative thinking out there, and part of our effort is aimed at getting the best minds engaged in privacy issues — many of them in this room — to meet and come up with the next great idea.

B. Lesson 2: It’s not (or shouldn’t be) in the fine print.

As we move forward on our plan to explore new privacy issues, we will continue to work with industry, academia, and the public to develop a comprehensive privacy framework that reflects the needs of the digital economy.

⁸ See Press Release, Truste Behavioral Advertising Survey, March 2009, http://truste-test.extractable.net/about_TRUSTE/press-room/news_truste_behavioral_targeting_survey.html.

We also recognize that transparency does not mean sticking a fine-print, leg

⁹ *In the Matter of Sears Holding Corp.*, FTC Docket No. C-4264 (September 9, 2009), <http://www.ftc.gov/os/caselist/0823099/index.shtm>.

innovative ways – outside of the privacy policy – to provide disclosures to consumers. For example, let’s say a consumer gets a targeted ad based on his or her search history. A company could provide an effective disclosure if it includes a link in close proximity to the ad, with the title “Why did I get this ad?” The text in the link could explain how data is collected for purposes of delivering targeted advertising. Indeed, such a disclosure is likely to be far more effective than a discussion – even a clear one – that is buried within a company’s privacy policy.

During our upcoming roundtables on privacy, we hope to hear more about innovative approaches to providing effective notice and choice, both online and offline. We also hope to hear directly from those who have done actual consumer testing

¹⁰ See Turow, King, Hoofnagle, Bleakley, and Hennessy, “Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It,” (September 2009), *available at* http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

¹¹ See George R. Milne, “Information Exchange Expectations of Consumers, Marketing Managers and Direct Marketers,” University of Massachusetts Amherst (presented on Nov. 1, 2007), *available at* <http://www.ftc.gov/bcp/workshops/ehavioral/presentations/3gmilne.pdf>.

See Federal Trade Commission, Self-Reg

Grisham online. But in certain cases, they may not want anyone to know their reading habits. To address this issue, I requested that Google disclose how it will use the personal information it collects when it offers books online and delivers targeted advertising to consumers. I further called upon Google to commit to complying with the FTC's self-regulatory principles for online behavioral advertising.¹³

The Commission also has recognized privacy as an important value in the health area. Recently, the Commission entered into a consent agreement with CVS Caremark Corporation, requiring the company to properly dispose of sensitive prescription information.¹⁴ As with the Google books example, I may or may not be harmed if people know that I take Percocet or Prednisone, but I still may want to keep that information private. Similarly, last month, the Commission's health breach notification rule went into effect. It requires certain web-based businesses to notify consumers about any breach of their individually identifiable health information, without regard to whether the breach caused tangible economic or other harm.¹⁵ The lesson we have learned from all of our work is this – privacy is simply an important value that we must work to protect. We will keep this lesson in mind as we move forward on our project to explore new privacy frameworks.

D. Lesson 4: Don't throw out the good with the bad.

The fourth lesson is that we shouldn't throw out the good out with the bad. In this

¹³ See Letter from David Vladeck to Jane Horvath Concerning the Google Books Project <http://www.ftc.gov/os/closings/090903horvathletter.pdf>.

¹⁴ See *In the Matter of CVS Caremark Corporation*, FTC Docket No. C-4259 (Jun. 18, 2009).

¹⁵ See www.ftc.gov/healthbreach.

context, the imperative to protect privacy should not deprive consumers of the benefits associated with information collection. For example, if we were to ban behavioral advertising altogether, consumers would not have access to much of the free online content they have come to expect.

When it comes to technology, we can't put the genie back in the bottle; nor would we want to. I touched on this subject at the beginning of my remarks – let's not go back to the days of encyclopedia research. Some of you can't imagine a world without the Internet, cell phones, or Blackberries, all of which permit the ubiquitous exchange of personal information. If we had been driven purely by fears of consumer privacy, none of these technologies would have flourished. Our policies must not discourage tomorrow's innovators.

E. Lesson 5: Keep up with the Joneses (or the Gates' and the Jobs')

Lesson 5 is that it really does pay to keep up with the online version of the proverbial Joneses; in this case, our policies need to keep up with the Gates' and the Jobs'. Put simply, our policies need to keep pace with rapidly-developing technology. This is a little different from Lesson 4, where I talked about the need to encourage new business models and technologies that benefit consumers. In addition to ensuring that our policies don't stifle innovation, we should ensure that the policies themselves do not become outdated.

addresses to be non-personally identifiable, it soon may be possible to link more IP addresses to specific individuals. In addition, even if certain items of information are anonymous by themselves, they can become identifiable when combined with other information. Professor LaTanya Sweeney from Carnegie Mellon University has estimated that 87% of the U.S. population can be uniquely identified if only a date of birth, gender and five-digit zip code are known. Thus, we can't just focus our policies on protecting people's names, Socia

¹⁶Hamblen, Matthew, "Privacy Algorithms," ComputerWorld (October 14, 2002).

held accountable to you. We look forward to working with you, and we especially look forward to seeing you in December.